

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-261217

(43)Date of publication of application : 03.10.1997

(51)Int.Cl.

H04L 9/10  
G09C 1/00  
G09C 1/00  
H04L 9/30  
H04L 9/32

(21)Application number : 08-072949

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 27.03.1996

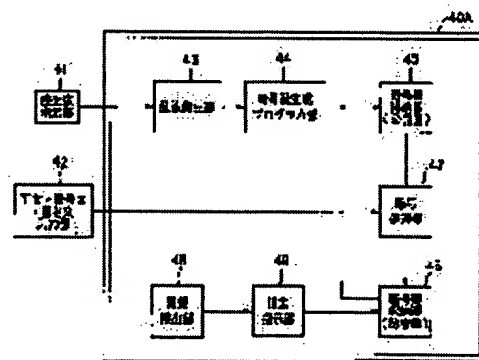
(72)Inventor : ISHII SHINJI

## (54) COMMUNICATION EQUIPMENT AND ITS METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To generate the key of an open key password without requiring a specified device by providing a means for generating an open key required to inspect a secret key necessary for a signature and the signature inside damper mechanism.

**SOLUTION:** In a device where ciphered digital data is received, the reception is proved by utilizing the digital signature and ciphered digital data is decoded and processed, a random number generating part 43 and a password key generating program part 44 generate the key of the open key password in accordance with an instruction from a key generation indicating part 41. An open key storing part 45 storing a decoding key for decoding ciphered digital data, a secret key storing part 46 storing a decoding key for decoding ciphered digital data and a password processing part 47 decoding ciphered digital data are arranged inside damper mechanism from which data is not taken out so as to prevent the illegal copying of digital data. The means for generating the necessary open key in order to inspect the secret key required for the signature and the signature is provided inside damper mechanism.



## LEGAL STATUS

17

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the  
examiner's decision of rejection or application  
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of  
rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

\* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]

[Claim 1] Receive the enciphered digital data and this reception is proved using a digital signature. A private key storage means to be equipment processed so that said enciphered digital data may be decoded and it may not be known by many persons, and to memorize a private key required for a signature, A decode key storage means to memorize the decode key which decodes the enciphered digital data, In the communication device which prevented the illegal copy of digital data when the ejection of data arranged an encryption data decode means to decode the enciphered digital data, in the impossible Tampa device The communication device characterized by establishing a key generation means to generate a public key required in order to verify a private key and a signature required for a signature, in the Tampa device.

[Claim 2] The communication device according to claim 1 characterized by using the information or the executive program encoded as digital data.

[Claim 3] The communication device according to claim 1 or 2 characterized by having the Tampa function, and to have been able to carry the private key storage means, the decode key storage means, and the key generation means, and having arranged them to a body in the case which can exchange data at least among the means belonging to the Tampa device.

[Claim 4] Although it can use where the encoded digital information is decoded, proving that surely the addressee received the information encoded by digital one which the origination side sent in the condition that an informational origination side and an informational receiving side are connected through the network, and In order to prevent from copying the digital information, the equipment of an origination side A transmitting-side encryption means to encipher the encoded digital information, and an encryption data transmitting means to send the enciphered digital information to a receiving side are provided. The equipment of a receiving side An encryption data receiving means to receive encryption data, and an encryption data decode means to decode the enciphered digital data, A coded data decode means to decode the encoded digital data, A connection means to connect an encryption data decode means and a coded data decode means, The Tampa device for playback for many persons not to know the digital data of a connection means, A decode key storage means to hold the decode key which decodes encryption data, and a signature means to prove having received the enciphered data using a digital signature, A key generation means to generate a public key required in order to verify a private key and a signature required for a signature, A private key storage means to memorize a private key required for a signature, and a public key output means to exhibit a public key required for verification of a signature, The communication device characterized by providing the Tampa device for keys for many persons not knowing the I/O result of a decode key storage means, a key generation means, and a private key storage means.

[Claim 5] Although proving surely the addressee having received the executive program which the origination side sent in the condition that an informational origination side and an informational receiving side are connected through the network, and the executive program which received can be performed In order to prevent from copying a program, the equipment of an origination side A transmitting-side encryption means to encipher an executive program, and an encryption data transmitting means to send the enciphered executive program to a receiving side are provided. The equipment of a receiving side An encryption data receiving means to receive encryption data, and an encryption executive program decode means to decode the enciphered executive program, A connection means to connect a program execution means to perform an executive program, and an encryption executive program decode means and a

program execution means, The Tampa device for program executions for many persons not to know the digital data after decode of a connection means, A decode key storage means to hold the decode key which decodes encryption data, and a signature means to prove having received the enciphered data using a digital signature, A key generation means to generate a public key required in order to verify a private key and a signature required for a signature, A private key storage means to memorize a private key required for a signature, and a public key output means to exhibit a public key required for verification of a signature, The communication device characterized by providing the Tampa device for keys for many persons not knowing the I/O result of a decode key storage means, a key generation means, and a private key storage means.

[Claim 6] the communication device according to claim 4 or 5 characterized by having provided the portable case equipped with the means belonging to the Tampa device for keys, and the equipment of the receiving side except the means belonging to the Tampa device for keys, and establishing an interface means of said case and equipment of a receiving side for it to be alike, respectively and to exchange data.

[Claim 7] Although it can use where the encoded digital information is decoded, proving that surely the addressee received the information encoded by digital one which the origination side sent in the condition that an informational origination side and an informational receiving side are connected through the network, and In order to prevent from copying the digital information, in a transmitting side Encipher the encoded digital information and the this enciphered digital information to a receiving side in delivery and a receiving side Receive encryption data through a network and many persons take care not to know decode of encryption, and the digital data of the part which decodes coding. It proves having held the key which decodes encryption data and having received the enciphered data using a digital signature. A public key required in order to verify a private key and a signature required for a digital signature is generated. Memorize a private key required for a signature and a public key required for verification of a signature is exhibited. The correspondence procedure characterized by decoding the enciphered digital data, decoding the encoded digital data, and many persons taking care not to know the decode key of digital data, the key generation for a signature, and the I/O result of the private key for a signature.

[Claim 8] Although it can use where an executive program is decoded as a procedure of an origination side, proving that surely the addressee received the executive program which the origination side sent in the condition that an informational origination side and an informational receiving side are connected through the network, and In order to prevent from copying the executive program, in a transmitting side Encipher an executive program and the enciphered executive program to a receiving side in delivery and a receiving side Receive encryption data through a network and many persons take care not to know decode of encryption, and the digital data of the part which performs an executive program. It proves having held the key which decodes encryption data and having received the enciphered data using a digital signature. A public key required in order to verify a private key and a signature required for a digital signature is generated. Memorize a private key required for a signature and a public key required for verification of a signature is exhibited. The correspondence procedure characterized by the thing for which the enciphered executive program is decoded, an executive program will be performed if required, and many persons get to know the decode key of digital data, the key generation for a signature, and the I/O result of the private key for a signature, and it is made for there not to be.

---

[Translation done.]

\* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the communication device which can generate the key of public key encryption, and its approach, without needing special equipment.

[0002]

[Description of the Prior Art] When it is going to sell the digital data which has copyright like voice and image information, or an executive program using a network, prevention of an illegal copy poses a problem with user authentication and a delivery check.

[0003] As an approach of solving user authentication, there is a method of using the public key encryption of digital cryptographic algorithm. Hereafter, public key encryption is described simply.

[0004] There are a common key cryptosystem algorithm (secret key cryptosystem algorithm) and a public-key-encryption algorithm in digital cryptographic algorithm.

[0005] Although a high-speed operation is possible for a common key cryptosystem algorithm, only both who communicate need to hold the common key secretly from using the same common key as an encryption key and a decode key. Since a key which is different in an encryption key and a decode lock is used for a public-key-encryption algorithm, it becomes unnecessary on the other hand, to deliver a key secretly like the common key of a common key cryptosystem algorithm by exhibiting the encryption key, although there is much computational complexity and it is unsuitable for high-speed processing compared with a common key cryptosystem algorithm.

[0006] However, with a public-key-encryption algorithm, since the encryption key is exhibited, everyone can create a cipher. For this reason, it is also necessary to prove who has enciphered and sent the correspondence enciphered and sent. Then, the partner authentication using a signature came to be thought.

[0007] There is RSA cryptograph as an example of representation of the public-key-encryption algorithm equipped with the partner authentication function. About cryptocommunication, this uses an encryption key, when enciphering, when using a decode key when decoding, and generating a signature, a decode key is used, and when verifying the signature, it uses an encryption key.

[0008] On the other hand, in order to encipher the digital data which should be delivered, it is almost the case that not public key encryption but a common key cryptosystem is used. The greatest reason is that the direction of a very high-speed common key cryptosystem is suitable for cipher processing of very big digital data compared with public key encryption.

[0009]

[Problem(s) to be Solved by the Invention] However, with the common key cryptosystem algorithm, both who communicate have to own the common private key. Then, it is common to attest a partner and to deliver the common private key used for a common key cryptosystem using public key encryption. However, a user's copy cannot be prevented only by it. Then, invention (Japanese Patent Application No. No. 155030 [ seven to ], Japanese Patent Application No. No. 159414 [ seven to ], Japanese Patent Application No. No. 204642 [ seven to ]) characterized by the ability to create an individual pocket device as who does not know the private key used for user authentication by using the Tampa device (equipment) was proposed. However, in these invention, there was a problem that the Tampa equipment for embedding a user's private key was needed for an individual pocket device.

[0010] The purpose of this invention is to offer the communication device which can generate the key of public key

encryption, and its approach, without needing special equipment.

[0011]

[Means for Solving the Problem] In this invention, in order to solve said technical problem, the enciphered digital data is received. A private key storage means to be equipment processed so that this reception may be proved using a digital signature, said enciphered digital data may be decoded and it may not be known by many persons, and to memorize a private key required for a signature, A decode key storage means to memorize the decode key which decodes the enciphered digital data, In the communication device which prevented the illegal copy of digital data when the ejection of data arranged an encryption data decode means to decode the enciphered digital data, in the impossible Tampa device A key generation means to generate a public key required in order to verify a private key and a signature required for a signature was established in the Tampa device.

[0012] - since his private key which everyone including him do not know, and the private key which only he owns are generable without a special dedicated device in the digital information selling system using a network -- even he who can perform a partner authentication function for his check and who purchased - digital copyright information can offer the system which cannot copy illegally.

[0013]

[Embodiment of the Invention] Hereafter, although the gestalt of operation of this invention is explained according to a drawing, in a public-key-encryption algorithm, it has a code function and an authentication function and explains here using the RSA cryptograph used most widely. In Addition, about Detail of RSA Cryptograph, They are Ikeno and Oyama Collaboration. It is Explained in Full Detail by "Chapter 6 RSA Public Key Encryption" Edited "Present Age Code Theory" One by Institute of Electronics, Information and Communication Engineers.

[0014] (The 1st gestalt) Drawing 1 shows the fundamental configuration of the whole system which gives its service using this invention, and, for ten, as for a network and 30, a contents server and 20 are [ a personal terminal and 40 ] individual pocket devices among drawing.

[0015] The contents server 10 offers service. The person using service makes contents distribute to the personal terminal 30 through a network 20 from the contents server 10 by inserting the individual pocket device 40 in the personal terminal 30, and operating this personal terminal 30.

[0016] that drawing 2 indicates the detail of the individual pocket device 40 to be -- it is -- the inside of drawing, and 41 -- the key generation directions section and 42 -- for the cryptographic key generator section, and 45 and 46, as for the cipher-processing section and 48, the cryptographic key storing section and 47 are [ a plaintext, a cipher and the signature sentence input section, and 43 / the random-number-generation section and 44 / an opening detecting element and 49 ] the elimination directions sections.

[0017] During said configuration, any persons can touch the interior, twist and cover the part except the key generation directions section 41, and a plaintext, a cipher and the signature sentence input section 42 (Tampa device), and it is in 40A. Even if it is the owner of a metaphor and this individual pocket device 40, it covers and 40A is opened by force, and if it is going to read the private key of RSA cryptograph saved inside, the opening detecting element 48 will detect opening and will eliminate internal confidential information electrically by the elimination directions section 49.

Moreover, if it opens so that it cannot rewrite in a different lock, either, it has manufactured so that the terminal of a semiconductor chip and wiring of a base which are used inside the individual pocket device 40 may also break.

[0018] The individual pocket device 40 is equipped with two input systems and one output system. One of input systems is the key generation directions section 41 of RSA cryptograph. This is the directions which will generate the public key and private key of the RSA cryptograph to be used from now on, before a user is going to receive service using this individual pocket device 40. The concrete example directed by the key generation directions section 41 is seed (seed) of the random number used in the random-number-generation section 43.

[0019] The seed who uses it here has a suitable approach to twist generating the same seed as about 2 times. For example, it is practical to use the input-statement character and its input time interval of keyboard entry. The inputted seed becomes a random number in the random-number-generation section 43, and is given to the cryptographic key generator section 44. The cryptographic key generator section 44 generates the key of RSA cryptograph. Since it is necessary to exhibit a public key among the keys of the RSA cryptograph generated in the cryptographic key generator section 44, it is stored in the public key storing section 45 which can be read from the exterior of the individual pocket device 40. On the other hand, the direction of a private key is stored in the private key storing section 46 so that it cannot read.

[0020] Preparation of the key used inside the individual pocket device 40 above is termination.

[0021] A parameter is inputted into another input system 42, i.e., a plaintext, a cipher, and the signature sentence input section, when receiving service, and decode of encryption/cipher of a plaintext, and a signature/verification are needed. The public key which a partner exhibits is used for encryption of the inputted plaintext, and verification of a signature sentence. It is calculated and outputted to verification of a cipher in the cipher-processing section 47 using the private key of the private key storing section 46.

[0022] Thus, anyone can convince him of the ability only of what owns the individual pocket device 40 to be used for the private key of the generated RSA cryptograph, and everyone can be convinced that nobody can know the value of a private key itself also including what owns the individual pocket device 40.

[0023] - which in other words was the technical problem of this invention -- even he who can perform a partner authentication function for his check and who purchased - digital copyright information can offer the system which cannot copy illegally, and, moreover, the private key used with the individual pocket device 40 can be realized without special equipment.

[0024] As an actual example of the individual pocket device 40, it is easily realizable using the IC card and PC card (PCMCIA) which are standardized.

[0025] Moreover, as an approach of using the contents actually decoded by the receiving side, there are some which were proposed by Japanese Patent Application No. No. 298702 [ six to ] and Japanese Patent Application No. No. 299940 [ six to ].

[0026] In addition, the key generation directions section 41, and a plaintext, a cipher and the signature sentence input section 42 may be formed in the personal terminal 30 side which inserts this device 40, and can also unify the personal terminal 30 and the individual pocket device 40.

[0027] Drawing 3 is a flow chart which shows the key generation procedure in an individual humanity news device.

[0028] First, the owner of the individual pocket device 40 directs key generation initiation (s1). With these directions, the individual pocket device 40 creates the seed for random numbers (s2). Then, a random number is generated using this (s3), a key generator is started (s4) and a key is generated. Since it is necessary to distribute a public key to a communications partner among the generated keys, it outputs from the individual pocket device 40 (s5). A public key is registered into a certificate issue engine etc., and if required, the owner of the individual pocket device 40 will distribute the public key for the outputted public key to a communications partner, after being recognized, reception (s6) and.

[0029] On the other hand, the individual pocket device 40 stores a private key in the private key read-out improper field of the individual pocket device 40 (s7), and ends key generation.

[0030] Drawing 4 is a flow chart which shows the key elimination procedure in an individual humanity news device.

[0031] In order that whether you are whom including the owner of the individual pocket device 40 may take out the confidential information inside the individual pocket device 40, the case where it is going to manipulate is assumed. It is thought that it tries whether to be able to take out a certain confidential information from the interface of the individual pocket device 40 and the personal terminal 30 at first. However, since it is not outputted except the information which can naturally be released, confidential information cannot be obtained. Then, when not giving up here, the inside of the individual pocket device 40 is opened and it is thought that it tries to take out confidential information.

[0032] if -- as much as possible -- the case of a device -- it is going to wrench it open (sp1) -- device opening is detected (sp2), a private key elimination program is started (sp3), and a private key is eliminated (sp4).

[0033] moreover, the individual pocket device 40 -- impossible -- wrenching it open (sp5) -- the carried main chips are destroyed (sp6) and informational ejection becomes impossible.

[0034] Thus, it is impossible, even if it is going to open the individual pocket device 40 even if and is going to obtain confidential information.

[0035]

[Effect of the Invention] As explained above, according to this invention, the personal private key which can carry out certification only whose user can use the private key of public key encryption which everyone cannot know can be generated using an individual pocket device, without using a special dedicated device.

[0036] When dealing with digital information as goods on a special network by using this individual pocket device, it is effective in the ability to prove now that it can prove that a user is only and, as for what paid and expressed volition, a

user cannot copy digital information to an information provider without notice.

---

[Translation done.]

\* NOTICES \*

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] The block diagram of the whole system which offers service using this invention

[Drawing 2] The block diagram showing the detail of an individual pocket device

[Drawing 3] The flow chart which shows the key generation procedure in an individual pocket device

[Drawing 4] The flow chart which shows the key elimination procedure in an individual pocket device

[Description of Notations]

10 [ -- An individual pocket device, 41 / -- The key generation directions section, 42 / -- A plaintext, a cipher and the signature sentence input section, 43 / -- The random-number-generation section, 44 / -- 45 The cryptographic key generator section, 46 / -- The cryptographic key storing section, 47 / -- The cipher-processing section, 48 / -- An opening detecting element, 49 / -- The elimination directions section, 40A / -- Cover. ] -- A contents server, 20 -- A network, 30 -- A personal terminal, 40

---

[Translation done.]

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-261217

(43)Date of publication of application : 03.10.1997

(51)Int.Cl.

H04L 9/10

G09C 1/00

G09C 1/00

H04L 9/30

H04L 9/32

(21)Application number : 08-072949

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 27.03.1996

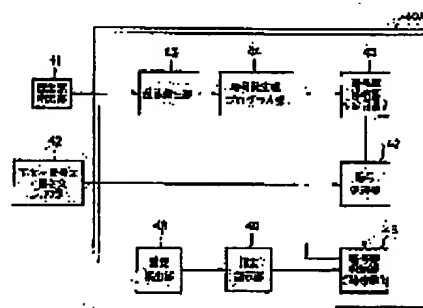
(72)Inventor : ISHII SHINJI

## (54) COMMUNICATION EQUIPMENT AND ITS METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To generate the key of an open key password without requiring a specified device by providing a means for generating an open key required to inspect a secret key necessary for a signature and the signature inside damper mechanism.

**SOLUTION:** In a device where ciphered digital data is received, the reception is proved by utilizing the digital signature and ciphered digital data is decoded and processed, a random number generating part 43 and a password key generating program part 44 generate the key of the open key password in accordance with an instruction from a key generation indicating part 41. An open key storing part 45 storing a decoding key for decoding ciphered digital data, a secret key storing part 46 storing a decoding key for decoding ciphered digital data and a password processing part 47 decoding ciphered digital data are arranged inside damper mechanism from which data is not taken out so as to prevent the illegal copying of digital data. The means for generating the necessary open key in order to inspect the secret key required for the signature and the signature is provided inside damper mechanism.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-261217

(43) 公開日 平成9年(1997)10月3日

(51) IntCl <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A
G 0 9 C 1/00	6 2 0	7259-5J	G 0 9 C 1/00	6 2 0 B
	6 4 0	7259-5J		6 4 0 B
H 0 4 L 9/30			H 0 4 L 9/00	6 6 3 B
9/32				6 7 5 B

審査請求 未請求 請求項の数 8 O L (全 7 頁)

(21) 出願番号 特願平8-72949

(22) 出願日 平成8年(1996)3月27日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 石井 晋司

東京都新宿区西新宿3丁目19番2号 日本

電信電話株式会社内

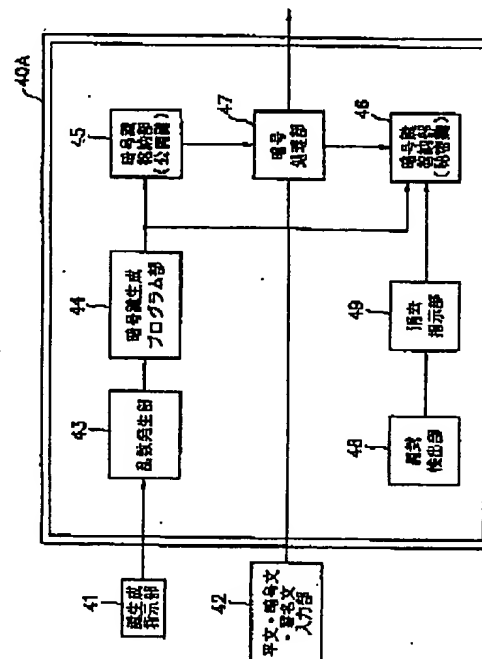
(74) 代理人 弁理士 吉田 精孝

(54) 【発明の名称】 通信装置及びその方法

(57) 【要約】

【課題】 特別な装置を必要とすることなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供すること。

【解決手段】 鍵生成指示部41からの指示に従って公開鍵暗号の鍵を生成する乱数発生部43及び暗号鍵生成プログラム部44と、該生成した鍵を格納する暗号鍵格納部45、46と、平文・暗号文・署名文入力部42から入力される平文または暗号文もしくは署名文を前記鍵を用いて暗号化または復号化もしくは署名する暗号処理部47とを、開封検出部48により開封を検出すると消去指示部49によって暗号鍵格納部46に格納した秘密鍵を消去する個人携帯デバイス40の被い40A内に設けておくことにより、該デバイス40がない限り情報を利用できないようにして不正コピーを防止する。



(2)

## 【特許請求の範囲】

【請求項1】 暗号化されたデジタルデータを受信し、該受信をデジタル署名を利用して証明し、前記暗号化されたデジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたデジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたデジタルデータを復号する暗号化データ復号手段とを、データの取り出しが可能なタンバ機構内に配置することによりデジタルデータの不正コピーを防止した通信装置において、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンバ機構内に設けたことを特徴とする通信装置。

【請求項2】 デジタルデータとして符号化された情報もしくは実行プログラムを用いたことを特徴とする請求項1記載の通信装置。

【請求項3】 タンバ機構に属する手段のうち少なくとも秘密鍵記憶手段と復号鍵記憶手段と鍵生成手段とを、タンバ機能を有しかつ携帯可能で本体に対しデータのやりとりが可能な筐体内に配置したことを特徴とする請求項1または2記載の通信装置。

【請求項4】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したデジタルに符号化された情報を受信者が確かに受信したことを証明することと、符号化されたデジタル情報を復号した状態で利用することはできるが、そのデジタル情報をコピーすることはできないようにするために、発信側の装置は、

符号化されたデジタル情報を暗号化する送信側暗号化手段と、

暗号化したデジタル情報を受信側に送る暗号化データ送信手段とを具備し、

受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、

暗号化されたデジタルデータを復号する暗号化データ復号手段と、

符号化されたデジタルデータを復号する符号化データ復号手段と、

暗号化データ復号手段と符号化データ復号手段とを連結する連結手段と、

連結手段のデジタルデータを何人にも知られないようにするための再生用タンバ機構と、

暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをデジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、

2

署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンバ機構とを具備したことを特徴とする通信装置。

【請求項5】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信した実行プログラムを受信者が確かに受信したことを証明することと、受信した実行プログラムを実行することはできるが、プログラムをコピーすることはできないようにするために、

発信側の装置は、

実行プログラムを暗号化する送信側暗号化手段と、

暗号化した実行プログラムを受信側に送る暗号化データ送信手段とを具備し、

受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、

暗号化された実行プログラムを復号する暗号化実行プログラム復号手段と、

実行プログラムを実行するプログラム実行手段と、

暗号化実行プログラム復号手段とプログラム実行手段とを連結する連結手段と、

連結手段の復号後のデジタルデータを何人にも知られないようにするためのプログラム実行用タンバ機構と、

暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをデジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、

署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンバ機構とを具備したことを特徴とする通信装置。

【請求項6】 鍵用タンバ機構に属する手段を備えた携帯可能な筐体と、鍵用タンバ機構に属する手段を除いた受信側の装置とを具備し、前記筐体と受信側の装置とのそれぞれにデータのやりとりを行うインタフェース手段を設けたことを特徴とする請求項4または5記載の通信装置。

【請求項7】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したデジタルに符号化された情報を受信者が確かに受信したことを証明することと、符号化されたデジタル情報を復号した状態で利用することはできるが、そのデジタル情報をコピーすることはできないようにするために、送信側では、

符号化されたデジタル情報を暗号化し、

(3)

3  
該暗号化したデジタル情報を受信側に送り、  
受信側では、  
ネットワークを介して暗号化データを受信し、  
暗号化の復号と符号化の復号を行う部分のデジタルデータ  
を何人にも知られないようにし、  
暗号化データを復号する鍵を保持し、  
暗号化されたデータを受信したことをデジタル署名を  
利用して証明し、  
デジタル署名に必要な秘密鍵及び署名を検証するため  
に必要な公開鍵を生成し、  
署名に必要な秘密鍵を記憶し、  
署名の検証に必要な公開鍵を公開し、  
暗号化されたデジタルデータを復号し、  
符号化されたデジタルデータを復号し、  
デジタルデータの復号鍵、署名用の鍵生成及び署名用の  
秘密鍵の入出力結果を何人にも知られないようにする  
ことを特徴とする通信方法。

【請求項8】 情報の発信側と受信側とがネットワーク  
を介して結ばれている状態にて、発信側が発信した実行  
プログラムを受信者が確かに受信したことを証明すること  
と、発信側の手順として実行プログラムを復号した状態  
で利用することはできるが、その実行プログラムをコ  
ピーすることはできないようにするために、  
送信側では、

実行プログラムを暗号化し、  
暗号化した実行プログラムを受信側に送り、  
受信側では、  
ネットワークを介して暗号化データを受信し、  
暗号化の復号と実行プログラムを実行する部分のデジ  
タルデータを何人にも知られないようにし、  
暗号化データを復号する鍵を保持し、  
暗号化されたデータを受信したことをデジタル署名を  
利用して証明し、  
デジタル署名に必要な秘密鍵及び署名を検証するため  
に必要な公開鍵を生成し、  
署名に必要な秘密鍵を記憶し、  
署名の検証に必要な公開鍵を公開し、  
暗号化された実行プログラムを復号し、  
必要ならば実行プログラムを実行し、  
デジタルデータの復号鍵、署名用の鍵生成及び署名用の  
秘密鍵の入出力結果を何人にも知られるないようにす  
ることを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、特別な装置を必要  
とすることなく公開鍵暗号の鍵を生成し得る通信装置及  
びその方法に関するものである。

【0002】

【従来の技術】音声・映像情報や実行プログラムのような  
著作権を有するデジタルデータを、ネットワークを

4  
利用して販売しようとする場合、利用者認証及び配送確  
認とともに不正コピーの防止が問題となる。

【0003】利用者認証を解決する方法としては、ディ  
ジタル暗号アルゴリズムの公開鍵暗号を利用する方法が  
ある。以下、公開鍵暗号について簡単にふれておく。

【0004】デジタル暗号アルゴリズムには、共通鍵  
暗号アルゴリズム（秘密鍵暗号アルゴリズム）と公開鍵  
暗号アルゴリズムとがある。

10 【0005】共通鍵暗号アルゴリズムは、高速演算が可  
能であるが、暗号化鍵と復号鍵に同じ共通鍵を使用する  
ことから、通信する両者のみがその共通鍵を秘密に保持  
する必要がある。一方、公開鍵暗号アルゴリズムは、共  
通鍵暗号アルゴリズムに比べて計算量が多く、高速処理  
には不向きであるが、暗号化鍵と復号鍵に異なる鍵を使  
用するため、暗号化鍵を公開しておくことにより、共通  
鍵暗号アルゴリズムの共通鍵のように鍵を秘密に配送す  
る必要がなくなる。

20 【0006】ところが、公開鍵暗号アルゴリズムでは、  
暗号化鍵を公開していることから誰もが暗号文を作成す  
ることができる。このため、暗号化されて送られてきた  
通信文等を、誰が暗号化して送ってきたかを証明するこ  
とも必要になる。そこで、考えられるようになったのが  
署名を利用した相手認証である。

【0007】相手認証機能を備えた公開鍵暗号アルゴリ  
ズムの代表例として、RSA暗号がある。これは暗号通  
信に関して、暗号化する時には暗号化鍵を利用し、復号  
する時には復号鍵を利用し、また、署名を生成する時は  
復号鍵を利用し、その署名を検証する時は暗号化鍵を利用  
するものである。

30 【0008】一方、配送すべきデジタルデータを暗号  
化するには、公開鍵暗号ではなく共通鍵暗号が使われる  
ことがほとんどである。その最大の理由は、非常に大き  
なデジタルデータの暗号処理には、公開鍵暗号に比べて  
極めて高速な共通鍵暗号の方が適しているからである。

【0009】

【発明が解決しようとする課題】しかし、共通鍵暗号アル  
ゴリズムでは、通信する両者が共通の秘密鍵を所有し  
ていなければならない。そこで、共通鍵暗号に使う共通  
の秘密鍵を公開鍵暗号を利用して相手を認証し、配送す  
ることが一般的である。しかし、それだけでは利用者の  
コピーは防ぐことはできない。そこで、利用者認証に用  
いる秘密鍵を、タンバ機構（装置）を用いることにより  
誰にも知られることのないようにして、個人携帯デバイ  
スを作成できることを特徴とした発明（特願平7-15  
5030号、特願平7-159414号、特願平7-2  
04642号）を提案した。しかし、これらの発明で  
は、個人携帯デバイスにユーザの秘密鍵を埋め込むため  
のタンバ装置が必要になるという問題があった。

50 【0010】本発明の目的は、特別な装置を必要とする

(4)

ことなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供することにある。

【0011】

【課題を解決するための手段】本発明では、前記課題を解決するため、暗号化されたデジタルデータを受信し、該受信をデジタル署名を利用して証明し、前記暗号化されたデジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたデジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたデジタルデータを復号する暗号化データ復号手段とを、データの取り出しが不能なタンバ機構内に配置することによりデジタルデータの不正コピーを防止した通信装置において、署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンバ機構内に設けた。

【0012】ネットワークを利用したデジタル情報販売システムでは、本人を含めて誰も知らない本人の秘密鍵と、本人しか所有していない秘密鍵を特別な専用装置なしに生成することができることから、本人の確認のために相手認証機能を行える、デジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができる。

【0013】

【発明の実施の形態】以下、図面に従って本発明の実施の形態を説明するが、ここでは公開鍵暗号アルゴリズムの中で暗号機能と認証機能を合わせ持ち、最も広く利用されているRSA暗号を用いて説明する。なお、RSA暗号の詳細については、池野、小山共著 社団法人電子情報通信学会編「現代暗号理論」の「第6章 RSA公開鍵暗号」に詳述されている。

【0014】（第1の形態）図1は本発明を利用してサービスを行うシステム全体の基本的な構成を示すもので、図中、10はコンテンツサーバ、20はネットワーク、30は個人用端末、40は個人携帯デバイスである。

【0015】コンテンツサーバ10はサービスを提供する。サービスを利用する者が、個人用端末30に個人携帯デバイス40を差し込み、該個人用端末30を操作することにより、コンテンツサーバ10からネットワーク20を介して個人用端末30にコンテンツを配布させる。

【0016】図2は個人携帯デバイス40の詳細を示すもので、図中、41は鍵生成指示部、42は平文・暗号文・署名文入力部、43は乱数発生部、44は暗号鍵生成プログラム部、45、46は暗号鍵格納部、47は暗号処理部、48は開封検出部、49は消去指示部である。

【0017】前記構成中、鍵生成指示部41及び平文・暗号文・署名文入力部42を除く部分は、いかなる者も

その内部に触れることができない被い（タンバ機構）40Aの中である。例えば、この個人携帯デバイス40の所有者であっても被い40Aを無理に開けて、内部に保存されているRSA暗号の秘密鍵を読み出そうとすると、開封検出部48が開封を検出し、消去指示部49により内部の秘密情報を電気的に消去する。また、違う鍵に書き換えたりすることもできないように、開封すると個人携帯デバイス40の内部で使用している半導体チップの端子や基盤の配線も壊れるように製造してある。

【0018】個人携帯デバイス40は、2つの入力系と1つの出力系を備えている。入力系のうちの1つはRSA暗号の鍵生成指示部41である。これは、ユーザがこの個人携帯デバイス40を利用してサービスを受けようとする前に、今後、使用するRSA暗号の公開鍵と秘密鍵を生成する指示である。鍵生成指示部41によって指示される具体的な例は、乱数発生部43で使用する乱数のシード（種）である。

【0019】ここで使用するシードはほぼ2度と同じシードを発生することのない方法がふさわしい。例えば、キーボード入力の入力文字とその入力時間間隔を利用するのが実用的である。入力されたシードは、乱数発生部43で乱数となり、暗号鍵生成プログラム部44に与えられる。暗号鍵生成プログラム部44はRSA暗号の鍵を生成する。暗号鍵生成プログラム部44で生成されたRSA暗号の鍵のうち、公開鍵は公開する必要があるので、個人携帯デバイス40の外部から読み出しが可能な公開鍵格納部45に格納される。一方、秘密鍵の方は読み出すことができないように秘密鍵格納部46に格納される。

【0020】以上で個人携帯デバイス40の内部で使用する鍵の準備は終了である。

【0021】サービスを受ける場合、平文の暗号化／暗号文の復号、署名／検証が必要になったときにパラメータがもう1つの入力系、つまり平文・暗号文・署名文入力部42に入力される。入力された平文の暗号化及び署名文の検証には、相手の公開する公開鍵を使用する。暗号文の検証には、秘密鍵格納部46の秘密鍵を利用して、暗号処理部47にて演算し出力される。

【0022】このようにして生成したRSA暗号の秘密鍵は、個人携帯デバイス40を所有するものだけが使用することができることを誰にでも納得させることができ、かつ秘密鍵の値そのものは個人携帯デバイス40を所有するものも含めて誰も知ることができないことを誰もが納得することができる。

【0023】言い換えると本発明の課題であった、本人の確認のために相手認証機能を行える、デジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができ、しかも、個人携帯デバイス40で使用する秘密鍵を特別な装置なしに実現することができる。

(5)

7

【0024】個人携帯デバイス40の実際の例としては、規格化されているICカード、PCカード（PCMCIA）を用いて容易に実現できる。

【0025】また、受信側で実際に復号したコンテンツを利用する方法としては、特願平6-298702号、特願平6-299940号で提案したものがある。

【0026】なお、鍵生成指示部41及び平文・暗号文・署名文入力部42は本デバイス40を差し込む個人用端末30側に設けても良く、また、個人用端末30と個人携帯デバイス40とを一体化することもできる。

【0027】図3は個人情報デバイスにおける鍵生成手順を示すフローチャートである。

【0028】最初に、個人携帯デバイス40の所有者が、鍵生成開始を指示する（s1）。この指示により、個人携帯デバイス40は乱数用シードを作成する（s2）。その後、これを利用して乱数を生成し（s3）、鍵生成プログラムを起動し（s4）、鍵を生成する。生成した鍵のうち、公開鍵は通信相手に配布する必要があるため、個人携帯デバイス40から出力する（s5）。出力された公開鍵を個人携帯デバイス40の所有者が受け取り（s6）、必要ならば、証明書発行機関などに公開鍵を登録し、承認された後、その公開鍵を通信相手に配布する。

【0029】一方、個人携帯デバイス40は、秘密鍵を個人携帯デバイス40の秘密鍵読み出し不可領域に格納し（s7）、鍵生成を終了する。

【0030】図4は個人情報デバイスにおける鍵消去手順を示すフローチャートである。

【0031】個人携帯デバイス40の所有者を含めた何者かが、個人携帯デバイス40の内部の秘密情報を取り出すために、細工をしようとする場合を想定する。最初は、個人携帯デバイス40と個人用端末30とのインタフェースから何らかの秘密情報が取り出せないかどうか試みると考えられる。しかしながら、当然公開可能な情報以外は出力されないため、秘密情報を得ることはできない。そこで、ここであきらめない場合、個人携帯デバイス40の中を開封し、秘密情報を取り出そうと試みる

8

と考えられる。

【0032】もし、少しでもデバイスのケースをこじ開けようとする（s p1）と、デバイス開封が検出され（s p2）、秘密鍵消去プログラムが起動されて（s p3）、秘密鍵が消去される（s p4）。

【0033】また、個人携帯デバイス40を無理にこじ開ける（s p5）と、搭載された主なチップが破壊され（s p6）、情報の取り出しは不可能となる。

【0034】このように、たとえ個人携帯デバイス40を開封し、秘密情報を得ようとしても不可能である。

【0035】

【発明の効果】以上説明したように、本発明によれば、個人携帯デバイスを用いて、誰もが知り得ない公開鍵暗号の秘密鍵をユーザのみが使用できる証明をすることができる個人用の秘密鍵を特別な専用装置を用いることなく生成することができる。

【0036】この個人携帯デバイスを使用することにより、特別なネットワーク上でデジタル情報を商品として取り扱う場合に、支払い意志を表明したものはユーザが唯一であることが証明でき、かつユーザがデジタル情報を情報提供者に無断でコピーできないことが証明できるようになる効果がある。

【図面の簡単な説明】

【図1】本発明を利用してサービスを提供するシステム全体の構成図

【図2】個人携帯デバイスの詳細を示す構成図

【図3】個人情報デバイスにおける鍵生成手順を示すフローチャート

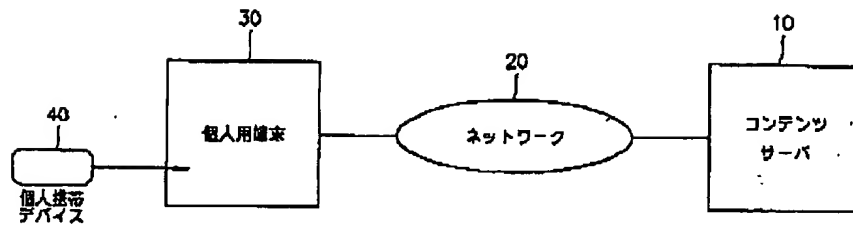
【図4】個人情報デバイスにおける鍵消去手順を示すフローチャート

【符号の説明】

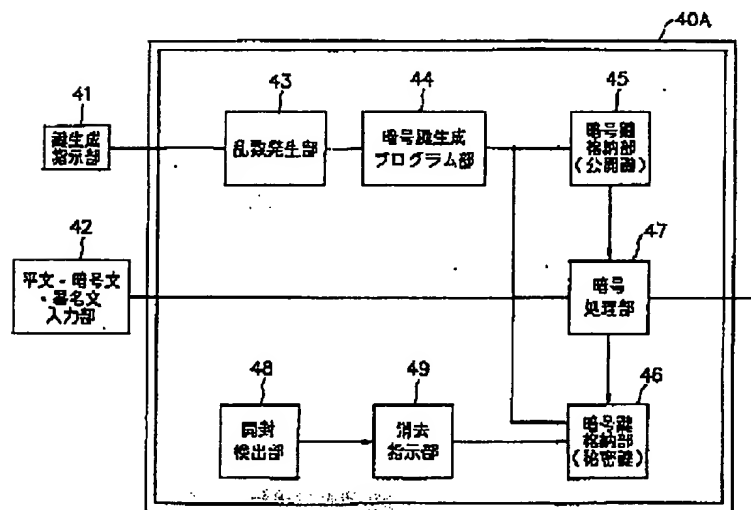
10…コンテンツサーバ、20…ネットワーク、30…個人用端末、40…個人携帯デバイス、41…鍵生成指示部、42…平文・暗号文・署名文入力部、43…乱数発生部、44…暗号鍵生成プログラム部、45、46…暗号鍵格納部、47…暗号処理部、48…開封検出部、49…消去指示部、40A…抜い。

(6)

【図1】

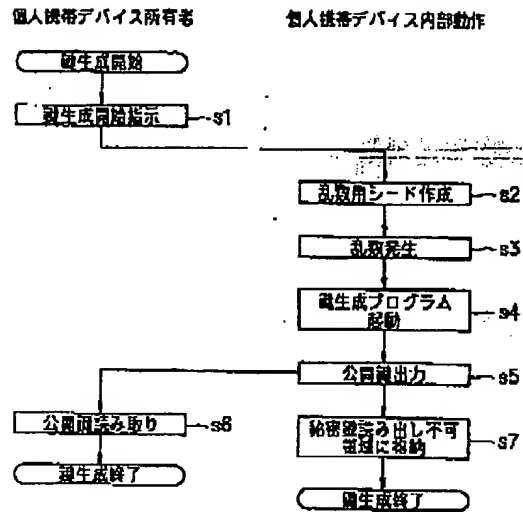


【図2】



(7)

【図3】



【図4】

